

## Patent Claims

1. Method for authenticating a data processing system,

5 according to which first information is generated by a first data processing system (16) and delivered to a second data processing system (14) of a control unit,

first data are transmitted from the second data processing system (14) to the first data processing system (16) over a data line, whereby the first data are generated by the  
10 second data processing system (14) with the aid of the first information and additional information contained in the second data processing system (14),

second data are generated by the first data processing system (16) depending on the first data and transmitted from the first data processing system (16) to the second data  
15 processing system (14) over the data line,

and according to which authentication information for authenticating the second data processing system (14) is generated by the second data processing system (14) with the aid of the second data.

20

2. Method according to claim 1, characterized in that the additional information contains a hardware identifier of the second data processing system (14).

3. Method according to claim 2, characterized in that a check [or: verification] is  
25 performed with the aid of the second data in order to determine whether the second data processing system (14) contains the hardware identifier.

4. Method according to one of the preceding claims, characterized in that the second data contain an expiration date and information based on which the access rights of  
30 the second data processing system (14) are defined.

5. Method according to claim 4, characterized in that the access rights are assigned with the aid of an authorization level.

6. Method according to one of the preceding claims, characterized in that the second data are transmitted in encrypted form.

5 7. Method according to one of the preceding claims, characterized in that the data line is a network connection, particularly a secure Internet connection.

8. Method according to one of the preceding claims, characterized in that the data connection is a point-to-point connection.

10 9. Method according to one of the preceding claims, characterized in that the second data contain a key (12).

15 10. Method according to one of the preceding claims, characterized in that the authenticity of the second data processing system (14) is verified by a third data processing system (40), which is contained in an electrophotographic printing or copying system.

20 11. Method according to one of the preceding claims, characterized in that the first information contains a transaction number.

12. Method according to one of the preceding claims, characterized in that the first information is sent per e-mail or mail.

25 13. Method according to claim 12, characterized in that the first information that is sent to the first data processing system (16) is entered by way of an input unit of the first data processing system (16).

30 14. Method according to one of the preceding claims, characterized in that the second data processing system (14) is a control unit, particularly for configuring, servicing, and operating an electrophotographic printing or copying system, whereby a third data processing system (40) of the printing or copying system verifies the authenticity of the second data processing system (14).

15. Method according to one of the preceding claims, characterized in that hardware information of the second data processing system (14) that cannot be modified by the user, particularly a serial number of a CPU or processor, is used as the hardware identifier of the second data processing system (14).

5

16. Method according to one of the preceding claims, characterized in that the second data are processed with the aid of an authentication procedure which generates third information, whereby the third information contains an expiration date and access rights of the second data processing system (14).

10

17. Method according to claim 16, characterized in that the authentication procedure generates the same third data in the processing of several second data of different second data processing systems (14).

15

18. Method according to one of the preceding claims, characterized in that the verification of the authenticity of the second data processing system (14) is performed with the aid of a challenge/response procedure.

20

19. Method according to one of the preceding claims, characterized in that the second data contain a signed certificate.

25

20. Method according to one of the preceding claims, characterized in that the second data contain a key, and the authentication information contains an authentication code that is generated with the aid of the key (12).

30

21. Arrangement for generating authentication information,

in which a first data processing system (16) generates first information, whereby the first information is delivered to a second data processing system (14) of a control unit,

the second data processing system (14) generates first data with the aid of the first information and additional information contained in the second data processing system (14),

a data line is provided over which first data are transmittable from the first data processing system (16) to the second data processing system (14),

5 the second data processing system (14) generates second data depending on the first data,

the second data are transmittable from the second data processing system (14) to the first data processing system (16) over the data line,

10 and in which the second data processing system (14), with the aid of the second data, generates authentication information for authenticating the second data processing system (40).

15 22. Method for authenticating a control unit of an electrophotographic printing or copying system,

according to which first data are stored in a first data processing system (14) of the control unit,

20 the first data processing system (14), with the aid of the first data, generates authentication information, which are transmitted to a second data processing system (40) of the printing or copying system with the aid of authentication data,

25 the authenticity of the first data processing system (14) is verified by the second data processing system (40),

and according to which method access rights of the first data processing system (14) are defined by the second data processing system (40) with the aid of the authentication data.

30

23. Method according to claim 22, characterized in that the first data contain a key (12) and/or signature.

24. Method according to claim 23, characterized in that the key (12) is a public key and/or a private key.

25. Method according to one of the claims 22 to 24, characterized in that the data are transmitted between the first data processing system (14) and the second data processing system (40) with the aid of a network connection, whereby the first data processing system (16) serves for remote control, remote servicing, and/or remote diagnostic analysis of the printing and/or copying system and has access at least to control units of the printing or copying system after the verification of authenticity.

26. Arrangement for authenticating a control unit of an electrophotographic printing or copying system,

in which a first data processing system (14) of the control unit contains first data,

the first data processing system (14) generates authentication information with the aid of the first data,

the first data processing system (14) transmits the authentication information to a second data processing system (40) of the printing or copying system with the aid of authentication data,

the second data processing system (40) verifies the authenticity of the first data processing system (14) with the aid of the authentication data,

and the second data processing system (40) defines access rights of the first data processing system (14) with the aid of the authentication data.